

ON MINKOWSKI PRODUCT SIZE: THE VOSPER'S PROPERTY

YAHYA OULD HAMIDOUNE

ABSTRACT. A subset S of a group G is said to be a Vosper's subset if $|A \cup AS| \geq \min(|G| - 1, |A| + |S|)$, for any subset A of G with $|A| \geq 2$. In the present work, we describe Vosper's subsets. Assuming that S is not a progression and that $|S^{-1}S|, |SS^{-1}| < 2|S|, |G'| - 1$, we show that there exist an element $a \in S$, and a non-null subgroup H of G' such that either $S^{-1}HS = S^{-1}S \cup a^{-1}Ha$ or $SHS^{-1} = SS^{-1} \cup aHa^{-1}$, where G' is the subgroup generated by $S^{-1}S$.

[2010]Primary 11P70; Secondary 20D60

Minkowski sum, Inverse theorems, Approximate groups, Cayley graphs

1. INTRODUCTION

Let A, B be subsets of a group G . The *Minkowski product* of A with B is defined as

$$AB = \{xy : x \in A \text{ and } y \in B\}.$$

Kneser's Theorem [15] states that AB is a periodic set if $|AB| \leq |A| + |B| - 2$ and if G is abelian. Diderrich [3] obtained the same conclusion assuming only that the elements of B commute. As mentioned in [10], the last result follows from Kneser's Theorem. In [17], Olson constructed subsets A and B of some non-abelian group with $|AB| \leq |A| + |B| - 2$ such that for every non-null group H ,

$$AB \neq AHB, AB \neq HAB \text{ and } AB \neq ABH.$$

The special cases $B = A$ and $B = A^{-1}$ received also some attention. In [4], Freiman described subsets A with $|A^2| < \frac{1+\sqrt{5}}{2}|A|$ or $|A^{-1}A| < \frac{1+\sqrt{5}}{2}|A|$. A transparent exposition of Freiman results is contained in Husbands dissertation [13].

Tao proposed in [20] a short proof of Freiman's result, suggesting that threshold should be 2. In [12], we obtained a Kneser type result, asserting that there exists a non-null subgroup H of G such that $A^{-1}HA = A^{-1}A$ or $AHA^{-1} = AA^{-1}$, if $|A^{-1}A| < 2|A| - 1$.

As mentioned by Tao, in [20], the relations $|A^{-1}A| < 2|A|$ and $|AA^{-1}| < 2|A|$ imply no kind of periodicity, since they are satisfied by left-progressions

in a torsion free group. The methods used in [12] are not enough precise to give an inverse theorem for $|A^{-1}A| < 2|A|$.

We need to develop the isoperimetric approach in the non-abelian case, continuing the work done in the finite case in [8]. The present work generalizes the results obtained in the abelian case [6] and the results obtained in the non-abelian finite case in [8, 9]. The two papers [6, 8] use the obsolete language of super-atoms. We use here the more general and more precise language of k -atoms introduced in [7]. Instead of restricting ourselves to the case of a Minkowski product, we develop the approach for an arbitrary relation. The information on Minkowski product will follow, once we restrict ourselves to Cayley relations $x^{-1}y \in A$. In almost all cases, the results obtained in the special case of Cayley relations hold for relations having a transitive group of automorphisms.

Among other tools, the isoperimetric approach, was used by Serra-Zemor [18] and by Vu-Wood [23] to replace the classical rectification. It was also used by the author [11] to propose a geometric approach to the classical Kemperman Theory [14], leading to simplifications and generalizations.

Let $\Gamma = (V, E)$ be a reflexive relation. The board of a subset X is $\Gamma(X) \setminus X$. Put $\mathbf{F}_k = \{X \subset V : |X| \geq k \text{ and } |V \setminus \Gamma(X)| \geq k\}$. The k th-connectivity κ_k is the minimal cardinality of the boards of the members of \mathbf{F}_k . A member of \mathbf{F}_k achieving this minimum will be called a k -fragment. A k -fragment with minimal (resp. maximal when V is finite) cardinality will be called a k -atom (resp. k -super-fragment). The relation will be called k -faithful if $|A| \leq |V \setminus \Gamma(A)|$, where A is a k -atom. A relation Γ will be called a Cauchy relation if $\kappa_1 \geq |\Gamma(v)| - 1$, for some $v \in V$. A relation with $\kappa_2 > \kappa_1$ will be called a Vosper's relation. In this language, the Cauchy-Davenport Theorem [1, 2] states that Cayley relations on groups with a prime order are Cauchy relations. Vosper's Theorem [22] states that, for $|G|$ a prime, the Cayley relation $x^{-1}y \in A$ is a Vosper's relation, if A is not an arithmetic progression.

Our main problem is to describe the Vosper's Cayley relations. The organization of the paper is the following:

Section 2 contains some terminology. The basic notions are presented in section 3. In Section 4, we prove that the intersection of distinct k -atoms of a k -faithful relation has cardinality less than k . We show also in this section that the intersection of distinct k -super-fragments has cardinality less than k , when the reverse relation is non- k -faithful. In section 5, we obtain more precise intersection properties for non Vosper's relations. In

section 6, we investigate the intersection of three 2-atoms. In section 7, we apply the last result to describe Vosper's relations with a transitive group of automorphisms. In section 8, we show that one of the two Cayley relations $x^{-1}y \in A$ and $x^{-1}y \in A^{-1}$ has 2-atom of the form $H \cup Ha$, where H is a subgroup and a is an element of G . As an application, we obtain in section 9, we obtain the following result:

Theorem 1.1. *Let A be a subset of group G_0 and let G be the subgroup generated by $A^{-1}A$. If $|A^{-1}A|, |AA^{-1}| < 2|A|$, then one of the following holds:*

- (i) *There is an $u \in G$ with $u^2 = 1$ such that either $AA^{-1} = G \setminus \{u\}$ or $A^{-1}A = G \setminus \{u\}$,*
- (ii) *A is a progression,*
- (iii) *there exists is a non-null subgroup H of G such that $A^{-1}HA = A^{-1}A \cup a^{-1}Ha$, for some $a \in A$,*
- (iv) *there exists is a non-null subgroup H of G such that $AHA^{-1} = AA^{-1} \cup aHa^{-1}$, for some $a \in A$.*

2. SOME TERMINOLOGY

An ordered pair $\Gamma = (V, E)$, where V is a set and $E \subset V \times V$, will be called a *graph* or a *relation* on V . Let $\Gamma = (V, E)$ be a graph and let $X \subset V$. The *reverse* graph of Γ is the graph $\Gamma^- = (V, E^-)$, where $E^- = \{(x, y) : (y, x) \in E\}$. The graph Γ will be called *locally-finite* if for all $x \in V$, $|\Gamma(x)|$ and $|\Gamma^-(x)|$ are finite. The graph Γ is said to be *r-regular* if $|\Gamma(x)| = r$, for every $x \in V$. The graph Γ is said to be *r-reverse-regular* if $|\Gamma^-(x)| = r$, for every $x \in V$. The graph Γ is said to be *r-bi-regular* if it is *r-regular* and *r-reverse-regular*.

- The minimal degree of Γ is defined as $\delta(\Gamma) = \min\{|\Gamma(x)| : x \in V\}$.
- We write $\delta_{\Gamma^-} = \delta_-(\Gamma)$.
- The board of X is defined as $\partial_{\Gamma}(X) = \Gamma(X) \setminus X$.
- The exterior of X is defined as $\nabla_{\Gamma}(X) = V \setminus \Gamma(X)$.
- We shall write $\partial_{\Gamma}^- = \partial_{\Gamma^-}$. This subset will be called the *reverse-board* of X .
- We shall write $\nabla_{\Gamma}^- = \nabla_{\Gamma^-}$.

When the context is clear, the reference to Γ will be omitted.

3. BASIC NOTIONS

In this section, we define the concepts of *kth-connectivity*, *k-fragment* and *k-atom* and prove some elementary properties of these notions.

A graph Γ will be called k -separable if there is a finite subset $X \subset V$, with $k \leq |X| < \infty$ and $k \leq |V \setminus \Gamma(X)|$. The k th-connectivity of a k -separable graph Γ (called k th-isoperimetric number in [7]) is defined as

$$(3.1) \quad \kappa_k(\Gamma) = \min\{|\partial(X)| : k \leq |X| < \infty \text{ and } k \leq |V \setminus \Gamma(X)|\}.$$

A finite subset X of V such that $k \leq |X| < \infty$, $k \leq |V \setminus \Gamma(X)|$ and $|\partial(X)| = \kappa_k(\Gamma)$ is called a k -fragment of Γ . A k -fragment with minimum cardinality is called a k -atom.

These notions were introduced in [7]. Let us now introduce more notions. A subset X of V will be called a k -semi-fragment of Γ if either X is a k -fragment or $\nabla(X)$ is a reverse k -fragment. A k -fragment of a finite graph having a maximal cardinality will be called a k -super-fragment. The graph Γ will be called k -faithful if $|A| \leq |\nabla(A)|$, where A is a k -atom.

A k -semi-fragment of Γ^- will be called a reverse- k -semi-fragment of Γ . A k -fragment of Γ^- will be called a reverse k -fragment of Γ . We shall write $\kappa_{-k}(\Gamma) = \kappa_k(\Gamma^-)$. The reference to Γ could be implicit.

Recall that $\kappa_k(\Gamma)$ is the maximal integer j such that for every finite subset $X \subset V$ with $|X| \geq k$, $|\Gamma(X)| \geq \min(|V| - k + 1, |X| + j)$.

The following lemma is immediate from the definitions:

Lemma 3.1. *Let $k \geq 2$ be an integer. A reflexive locally finite k -separable graph $\Gamma = (V, E)$ is a $k - 1$ -separable graph, and moreover $\kappa_{k-1} \leq \kappa_k$. If $\kappa_{k-1} = \kappa_k$, then*

$$\mathbf{F}_k = \{F \in \mathbf{F}_{k-1} : k \leq \min(|F|, |\nabla(F)|)\}.$$

The next lemma contains useful duality relations:

Lemma 3.2. *Let X and Y be k -fragments of a reflexive locally finite k -separable graph $\Gamma = (V, E)$. Then*

$$(3.2) \quad \partial^-(\nabla(X)) = \partial(X),$$

$$(3.3) \quad \nabla^-(\nabla(X)) = X,$$

$$(3.4) \quad X \subset Y \text{ if and only if } \nabla(Y) \subset \nabla(X).$$

In particular, $\nabla(X)$ is a reverse- k -semi-fragment.

Proof. Clearly, $\partial(X) \subset \partial^-(\nabla(X))$

We must have $\partial(X) = \partial^-(\nabla(X))$, since otherwise there is a $y \in \partial^-(\nabla(X)) \setminus \partial(X)$. It follows that $|\partial(X \cup \{y\})| \leq |\partial(X)| - 1$, contradicting the definition of κ_k . This proves (3.2). In particular, $\nabla(X)$ is a reverse- k -semi-fragment.

Thus $\Gamma^-(\nabla(X)) = \nabla(X) \cup \partial^-(\nabla(X)) = \nabla(X) \cup \partial(X) = V \setminus X$. Thus (3.3) holds. Clearly, (3.4) is a direct consequence of (3.3). \square

Let us define two important notions:

Let $\Gamma = (V, E)$ be a reflexive graph. We shall say that Γ is a *Cauchy graph* if Γ is non-1-separable or if Γ has a 1-atom A with $|A| = 1$ or $|\nabla(A)| = 1$. We shall say that Γ is a *reverse-Cauchy graph* if Γ^- is a Cauchy graph.

Clearly, Γ is a Cauchy graph if and only if for every $X \subset V$ with $|X| \geq 1$,

$$|\Gamma(X)| \geq \min(|V|, |X| + \delta - 1).$$

We shall say that Γ is *degenerate* if Γ is 2-separable and $\kappa_2 = \kappa_1$. We shall say that Γ is *reverse-degenerate* if Γ^- is degenerate.

Lemma 3.3. *Let $\Gamma = (V, E)$ be a reflexive finite k -separable graph and let X be a subset of V . Then*

$$(3.5) \quad \kappa_k = \kappa_{-k}.$$

Moreover,

- (i) X is a k -fragment if and only if $\nabla(X)$ is a k -reverse-fragment,
- (ii) X is a k -super-fragment if and only if $\nabla(X)$ is a k -reverse-atom,
- (iii) Γ is a Cauchy graph if and only if it is a reverse-Cauchy graph,
- (iv) Γ is degenerate if and only if it is reverse-degenerate.

Proof. Observe that a finite graph is k -separable if and only if its reverse is k -separable. Take a k -fragment X of Γ . We have clearly $\partial_-(\nabla(X)) \subset \partial(X)$. Therefore

$$\kappa_k(\Gamma) \geq |\partial(X)| \geq |\partial_-(\nabla(X))| \geq \kappa_{-k}.$$

The reverse inequality of (3.5) follows similarly or by duality.

Suppose that X is a k -fragment. By (3.2) and (3.5), $|\partial_-(\nabla(X))| = |\partial(X)| = \kappa_k = \kappa_{-k}$, and hence $\nabla(X)$ is a reverse k -fragment. The other implication of (i) follows similarly. Suppose now that X is a k -super-fragment. By (i), $\nabla(X)$ is a reverse- k -fragment. Take a reverse- k -atom N . Now $\nabla^-(N)$ is a k -fragment by (i). Thus $|\nabla^-(N)| \leq |X|$, and hence using (3.3), $|\nabla(X)| \leq |N|$. Thus, $\nabla(X)$ is a reverse- k -atom. The other implication of (ii) follows similarly. Now (iii) and (iv) follow directly from the definitions and (3.5). \square

Recall the following easy fact:

Lemma 3.4. [7] *Let $\Gamma = (V, E)$ be a locally-finite k -separable graph and let A be a k -atom with $|A| > k$. Then $\Gamma^-(x) \cap A \neq \{x\}$, for every $x \in A$.*

Proof. We can not have $\Gamma^-(x) \cap A = \{x\}$, otherwise $A \setminus \{x\}$ would be a k -fragment. \square

4. GEOMETRIC PROPERTIES OF FRAGMENTS

The next result generalizes results obtained in [8, 7, 10]:

Theorem 4.1. *Let X be a k -fragment of a reflexive locally finite k -separable graph $\Gamma = (V, E)$ and let Y be a k -semi-fragment.*

- (i) *If $|X \cap Y| \geq k$, then $|\nabla(Y) \cap \partial(X)| \leq |X \cap \partial(Y)|$,*
- (ii) *If $|X \cap Y| \geq k$ and $|\nabla(X) \cap \nabla(Y)| \geq k$, then $X \cap Y$ is a k -fragment*
- (iii) *If $|X \cap Y| \geq k$ and $|X| \leq |\nabla(Y)|$, then $X \cap Y$ is a k -fragment*

Proof.

\cap	Y	$\partial(Y)$	$\nabla(Y)$
X	R_{11}	R_{12}	R_{13}
$\partial(X)$	R_{21}	R_{22}	R_{23}
$\nabla(X)$	R_{31}	R_{32}	R_{33}

Assume that $|X \cap Y| \geq k$. By the definition of κ_k ,

$$\begin{aligned}
 |R_{21}| + |R_{22}| + |R_{23}| &= \kappa_k \\
 &\leq |\partial(X \cap Y)| \\
 &= |R_{12}| + |R_{22}| + |R_{21}|,
 \end{aligned}$$

and hence $|\nabla(Y) \cap \partial(X)| = |R_{23}| \leq |R_{12}| = |X \cap \partial(Y)|$, showing (i).

We shall prove that

$$(4.1) \quad \text{If } |\nabla(X) \cap \nabla(Y)| \geq k, \text{ then } |\nabla(Y) \cap \partial(X)| \geq |X \cap \partial(Y)|,$$

Assuming that $|\nabla(X) \cap \nabla(Y)| \geq k$,

Case 1: Y is finite.

$$\begin{aligned}
 |R_{12}| + |R_{22}| + |R_{32}| &= \kappa_k \\
 &\leq |\partial(X \cup Y)| \\
 &\leq |R_{22}| + |R_{23}| + |R_{32}|,
 \end{aligned}$$

and hence $|R_{12}| \leq |R_{23}|$, showing (4.1) in this case.

Case 2: Y is infinite.

$$\begin{aligned}
 |R_{12}| + |R_{22}| + |R_{32}| &= \kappa_{-k} \\
 &\leq |\partial^-(R_{33})| \\
 &\leq |R_{22}| + |R_{23}| + |R_{32}|,
 \end{aligned}$$

and hence $|R_{12}| \leq |R_{23}|$, showing (4.1) in this case.

Assume now that $|X \cap Y| \geq k$ and $|\nabla(X) \cap \nabla(Y)| \geq k$. By (i) and (4.1), we have $|\nabla(Y) \cap \partial(X)| = |X \cap \partial(Y)|$. It follows that

$$\kappa_k \leq |\partial(X \cap Y)| \leq |R_{12}| + |R_{22}| + |R_{21}| \leq |R_{12}| \leq |R_{23}| + |R_{22}| + |R_{21}| = \kappa_k,$$

showing that $X \cap Y$ is a k -fragment.

Assume now that $|X \cap Y| \geq k$ and $|X| \leq |\nabla(Y)|$. By (i), $|R_{12}| \geq |R_{23}|$. Clearly,

$$|R_{13}| + |R_{23}| + R_{33} = |\nabla(Y)| \geq |X| = |R_{11}| + |R_{12}| + R_{13}.$$

Therefore $|\nabla(X) \cap \nabla(Y)| \geq |X \cap Y| \geq k$. Now, (iii) by applying (ii). \square

We shall now investigate the super-fragments behavior when the atoms are too big. Let us mention two easy facts:

Lemma 4.2. *A k -separable graph $\Gamma = (V, E)$ is either k -faithful or reverse k -faithful. Moreover infinite graphs are k -faithful.*

Proof. Assume that $\Gamma = (V, E)$ is non- k -faithful. Then V is clearly finite. Let A' be a reverse k -atom. By Lemma 3.3, $\nabla^-(A')$ is a k -fragment and $\nabla(A)$ is a reverse k -fragment. By (3.4), we have $|\nabla^-(A')| \geq |A| > |\nabla(A)| \geq |A'|$. In particular Γ is reverse-faithful. \square

Theorem 4.3. *Let $\Gamma = (V, E)$ be a reflexive finite k -separable graph such that Γ^- is a non- k -faithful graph. Then*

- (i) *the intersection of two distinct k -super-fragments has a cardinality less than k .*
- (ii) *Moreover, if $k \geq 2$ and $\kappa_k = \kappa_{k-1}$, then the intersection of two distinct k -super-fragments has a cardinality less than $k - 1$.*

Proof. Let X and Y be k -super-fragments of Γ . By Lemma 3.3, $\nabla(X)$ and $\nabla(Y)$ are reverse k -atoms of Γ . Since Γ^- is non- k -faithful, we have by (3.3), $|\nabla(X)| > |\nabla^-(\nabla(X))| = |X|$.

Suppose that $|X \cap Y| \geq k$. By Theorem 4.1,(iii), $X \cap Y$ is a k -fragment and hence $X = Y$, a contradiction.

Assume now that $\kappa_k = \kappa_{k-1}$ and that $|X \cap Y| \geq k - 1$. By Lemma 3.1, X and Y are $k - 1$ -fragments.

By Theorem 4.1,(i), $|\nabla(Y) \cap \partial(X)| \geq |X \cap \partial(Y)|$. Thus,

$$\begin{aligned} k - 1 &\leq |X \cap Y| = |X| - |X \cap \partial(Y)| - |X \cap \nabla(Y)| \\ &\leq |\nabla(Y)| - 1 - |\nabla(Y) \cap \partial(X)| - |X \cap \nabla(Y)| \\ &= |\nabla(X) \cap \nabla(Y)| - 1. \end{aligned}$$

By Theorem 4.1,(ii), applied to Γ^- , $\nabla(X) \cap \nabla(Y)$ is a $k - 1$ -reverse-fragment. By Lemma 3.1, $\nabla(X) \cap \nabla(Y)$ is a k -reverse-fragment. Thus, $\nabla(X) = \nabla(Y)$, and hence $X = Y$, a contradiction. \square

5. DEGENERATE GRAPHS

The next consequence of Theorem 4.1 will be a main tool:

Theorem 5.1. *Let A be a 2-atom of a reflexive locally finite 2-faithful degenerate graph $\Gamma = (V, E)$ and let X be a 2-semi-fragment not containing A . Then $|A \cap X| < 2$, if one of the following conditions holds:*

- (i) $|A| \leq \nabla(X)$,
- (ii) $\nabla(A) \cap \nabla(X) \neq \emptyset$.

In particular, the intersection of two distinct 2-atoms of a 2-faithful graph has a cardinality less than 2.

Proof. (i) follows by Theorem 4.1,(ii). Assume that $|A \cap X| \geq 2$ and $\nabla(A) \cap \nabla(X) \neq \emptyset$. Since $\kappa_2 = \kappa_1$ and by Lemma 3.1, A is a 1-fragment and X is a 1-semi-fragment. By Theorem 4.1,(ii), applied with $k = 1$, $A \cap X$ is a 1-fragment. By Lemma 3.2, $|\nabla(A \cap X)| \geq |\nabla(A)| \geq 2$. Thus, $A \cap X$ is a 2-fragment, and hence $A \cap X = A$, a contradiction. \square

Lemma 5.2. *Let X and Y be two 2-atoms of a reflexive locally finite 2-faithful degenerate graph $\Gamma = (V, E)$. Then*

$$(5.1) \quad |\partial(X \cap Y)| \leq |\Gamma(X) \cap \Gamma(Y)| - |X \cap Y| \leq \kappa_2, \text{ and}$$

$$(5.2) \quad |\nabla(X) \setminus \nabla(Y)| \leq |Y \setminus X| + \kappa_2 - |\partial(X \cap Y)|.$$

Proof. We use the notations of the proof of Theorem 4.1. By Lemma 3.1, X and Y are 1-fragments. We shall show that

$$(5.3) \quad |R_{12}| \geq |R_{23}|.$$

This holds by (4.1), applied with $k = 1$, if $|\nabla(X) \cap \nabla(Y)| \geq 1$. Suppose that $|\nabla(X) \setminus \nabla(Y)| = 0$. We have

$$|R_{11}| + |R_{12}| + |R_{13}| = |X| \leq |\nabla(X)| = |\nabla(Y)| = |R_{13}| + |R_{23}|,$$

and (5.3) holds. Thus

$$\begin{aligned} |\partial(X \cap Y)| &\leq |\Gamma(X) \cap \Gamma(Y)| - |X \cap Y| \\ &= |R_{12}| + |R_{22}| + |R_{12}| \\ &\leq |R_{23}| + |R_{22}| + |R_{12}| = \kappa_2, \end{aligned}$$

proving (5.1).

By Theorem 5.1, $|X \cap Y| = 1$. Also we have,

$$|\nabla(Y) \setminus \nabla(X)| = |R_{13}| + |R_{23}| \leq |R_{13}| + |R_{12}| = |X \setminus Y| = |X| - 1,$$

proving (5.2). \square

6. A DESCRIPTION OF THE 2-ATOMS

Theorem 6.1. *Let $\Gamma = (V, E)$ be a reflexive locally finite degenerate and reverse degenerate graph such that Γ and Γ^- are 2-faithful graphs. Then one of the following holds:*

- (i) *no vertex is incident to three pairwise distinct 2-atoms and incident to three pairwise distinct reverse-2-atoms.*
- (ii) *the 2-atom has cardinality 2 or the reverse-2-atom has cardinality 2.*

Proof. Let H be a 2-atom and let K be a reverse-2-atom. Without loss of generality we may take $|K| \geq |H|$.

Assume that (i) does not hold. We may choose two distinct 2-atoms X, Y incident to the same vertex v , since (i) does not hold. By Theorem 5.1, we have $X \cap Y = \{v\}$.

We have $\nabla(X) \not\subset \nabla(Y)$, by Lemma 3.2. Take $w \in \nabla(X) \setminus \nabla(Y)$. We have by (5.1), applied with X and Y permuted,

$$(6.1) \quad |\nabla(X) \setminus \nabla(Y)| \leq |Y| - 1.$$

Case 1: $L_1 \cup L_2 \subset \nabla(X)$, for some distinct reverse-2-atoms L_1 and L_2 with $w \in L_1 \cap L_2$. By Theorem 5.1, $L_1 \cap L_2 = \{w\}$. By Lemma 3.2, $\nabla(Y)$ is a reverse-2-semi-fragment and $X \subset \nabla^-(L_1) \cap \nabla^-(L_2)$. Take an arbitrary $i \in \{1, 2\}$. Since $w \in L_i$, we have $L_i \not\subset \nabla(Y)$. Since $X \subset \nabla^-(L_i)$, we have $v \in \nabla^-(L_i) \cap Y$. By Theorem 5.1, (ii), $|L_i \cap \nabla(Y)| \leq 1$.

We have using (6.1),

$$2|Y| - 3 \leq 2|K| - 3 \leq |(L_1 \cup L_2) \setminus \nabla(Y)| \leq |\nabla(X) \setminus \nabla(Y)| \leq |Y| - 1,$$

and hence $|X| = 2$. Thus (ii) holds.

Case 2: $\nabla(X)$ contains at most one reverse-2-atom.

Since (ii) fails, there exist three pairwise distinct reverse-2-atoms containing w . We can now assume without loss of generality that there are distinct reverse-2-atoms L, M with $w \in L \cap M$ and

$$L, M \not\subset \nabla(X).$$

By Lemma 3.2, $X \not\subset \nabla^-(L)$, and $X \not\subset \nabla^-(M)$.

We have $|X \cap \nabla^-(L)| \leq 1$ and $|X \cap \nabla^-(M)| \leq 1$, by Theorem 5.1, (i). It follows that

$$|X \cap \Gamma^-(L) \cap \Gamma^-(M)| \geq |X| - 2.$$

By (5.1), we have

$$(6.2) \quad |\Gamma^-(L) \cap \Gamma^-(M)| \leq 1 + \kappa_{-2} = 1 + \kappa_{-1}.$$

Since $w \in \nabla(X)$, we have $\Gamma^-(w) \subset \Gamma^-(\nabla(X)) = V \setminus X$. Now we have

$$\begin{aligned} 1 + \kappa_{-1} + |X| - 2 &\leq |\Gamma^-(w)| + |X| - 2 \\ &\leq |\Gamma^-(w)| + |X \cap (\nabla^-(L) \cup \nabla^-(M))| \\ &\leq |\Gamma^-(L) \cap \Gamma^-(M)| \leq 1 + \kappa_{-1} \end{aligned}$$

and hence $|X| = 2$. \square

For self-reverse-graphs, this result becomes Theorem 9.3 of [10], where the hypothesis self-reverse is omitted. The reader may suspect this, since Corollaries 9.4 and 9.6 are self-reverse. Also the finite case of this result is proved in [9].

7. VERTEX-TRANSITIVE GRAPHS

Let $\Gamma = (V, E)$ be a graph. A function $f : V \rightarrow V$ will be called a *homomorphism* if for all $x \in V$, we have $\Gamma(f(x)) = f(\Gamma(x))$. A bijective homomorphism is called an *automorphism*. The graph Γ will be called *vertex-transitive* if for all $x, y \in V$, there is an automorphism f such that $y = f(x)$. Clearly a vertex-transitive graph is regular. It is bi-regular if V is finite. A *block* of Γ is a subset $B \subset V$ such that for every automorphism f of Γ , either $f(B) = B$ or $f(B) \cap B = \emptyset$.

The objects defined in the previous sections (fragments, atoms and super-fragments) are defined using the graph structure. Therefore the image of any of these objects by a graph automorphism is an object with the same kind. This trivial observation will be used without any reference.

Recall the following result:

Theorem 7.1. [8] *Let $\Gamma = (V, E)$ be a reflexive locally finite 1-separable vertex-transitive graph. There is a block which is either a 1-atom or a reverse-1-atom. In particular a graph is a Cauchy graph if and only if its block boards and block reverse-boards have size greater than $\delta - 2$.*

Proof. By Lemma 4.2, Γ is 1-faithful or reverse-1-faithful. If Γ is 1-faithful, the 1-atom is a block, by Theorem 5.1. If Γ is reverse-1-faithful, the reverse 1-atom is a block, by Theorem 5.1. \square

Theorem 7.2. *Let $\Gamma = (V, E)$ be a reflexive locally finite vertex-transitive graph such that Γ is degenerate and reverse-degenerate. Then one of the following holds:*

- (i) *One of the graphs Γ and Γ^- is not a Cauchy graph and either the 1-atom or the reverse 1-atom is a block,*

- (ii) *One of the graphs Γ and Γ^- is non-2-faithful and its reverse-2-super-fragment is a block,*
- (iii) *The graphs Γ and Γ^- are 2-faithful Cauchy graphs and no vertex is incident to three distinct 2-atoms and to three distinct reverse-2-atoms.*
- (iv) *The 2-atoms or the reverse-2-atom have cardinality 2.*

Proof. By the assumptions of the theorem, we have $\kappa_2 \leq \delta - 1$. Consider first the case, where Γ is not a Cauchy graph. By Theorem 7.1, the 1-atom is a block or the reverse-1-atom is a block, and thus (i) holds. Similarly the result holds if Γ^- is not a Cauchy graph. From now on, we shall assume that the graphs Γ and Γ^- are Cauchy graphs.

We have $\delta - 1 \geq \kappa_2 \geq \kappa_1 = \delta - 1$. Similarly, $\delta_- - 1 \geq \kappa_{-2} \geq \kappa_{-1} = \delta_- - 1$.

Assume first that one of the graphs Γ and Γ^- is non-faithful. Then its reverse-2-super-fragment is a block, by Theorem 4.3,(ii). Assume now that the graphs Γ and Γ^- are faithful and that (iv) does not hold. By Theorem 6.1, some vertex is incident to at most two distinct 2-atoms, or to at most two distinct reverse-2-atoms, and hence (iii) holds. Since Γ is vertex-transitive, no vertex is incident to three distinct 2-atoms and to three distinct reverse-2-atoms, and hence (iii) holds. \square

Using Lemma 3.3, we get:

Corollary 7.3. [8] *Let $\Gamma = (V, E)$ be a finite reflexive degenerate vertex-transitive graph. Then one of the following holds:*

- (i) *The graphs Γ is not a Cauchy graph and either the 1-atom or the reverse 1-atom is a block,*
- (ii) *One of the graphs Γ and Γ^- is non-faithful and its reverse-2-super-fragment is a block,*
- (iii) *The graphs Γ and Γ^- are 2-faithful Cauchy graphs and no vertex is incident to three distinct 2-atoms and to three distinct reverse-2-atoms.*
- (iv) *The 2-atoms or the reverse-2-atom have cardinality 2.*

8. CAYLEY GRAPHS

Let G be a group. A *right- r -progression* is a set of the form $\{a, ra, \dots, r^j a\}$, for some $r \in G$. A *left- r -progression* is a set of the form $\{a, ar, \dots, ar^j\}$, for some $r \in G$. A set will be called an *r -progression* if it is either a right r -progression or a left r -progression.

Let S be a subset of G . The subgroup generated by S will be denoted by $\langle S \rangle$. The graph (G, E) , where $E = \{(x, y) : x^{-1}y \in S\}$ is called a *Cayley graph*. It will be denoted by $\text{Cay}(G, S)$. Put $\Gamma = \text{Cay}(G, S)$ and let $F \subset G$. Clearly $\Gamma(F) = FS$, where $FS = \{xy : x \in F \text{ and } y \in S\}$ is the Minkowski product of F by S . One may check easily that left-translations are automorphisms of Cayley graphs. In particular, Cayley graphs are bi-regular and vertex-transitive.

Recall the following easy fact:

Lemma 8.1. [6] *Let G be group and let S be finite generating subset with $1 \in S$. For every $a \in S$, $\langle S \rangle = \langle Sa^{-1} \rangle$. Moreover $\text{Cay}(G, Sa^{-1})$ and $\text{Cay}(G, S)$ have the same k -fragments. The left-translation of a k -atom (resp. k -fragment) is a k -atom (resp. k -fragment).*

The proof follows by an easy verification. The last part can be done directly, by observing that left translations are Cayley graph automorphisms.

The next lemma allows translating intersection properties into coset covering:

Lemma 8.2. *Let A be a subset of a group G . Put $t = |\{x^{-1}A : a \in A\}|$. Then A is the union of t right Q -cosets, where $Q = \{x : xA = A\}$.*

The following result generalizes a theorem of Mann [16] in the abelian case:

Theorem 8.3. [8] *Let G be group and let S be finite generating subset with $1 \in S$ and assume that the graph $\Gamma = \text{Cay}(G, S)$ is 1-separable. Then the 1-atom containing 1 is a subgroup or the reverse 1-atom containing 1 is a subgroup. Then Γ a cauchy graph if and only, for every finite subgroup H , $\min(|HS|, |SH|) \leq \min(|G|, |H| + |S| - 1)$.*

Proof. The result follows by combining Lemma 8.2 and Theorem 7.1. \square

We are now ready to show that either the 2-atoms have a nice structure or the 2-super-fragments have structure in the degenerate case.

Theorem 8.4. *Let G be group and let S be finite generating subset with $1 \in S$ and put $\Gamma = \text{Cay}(G, S)$. Also assume that Γ is degenerate and reverse-degenerate. Then there are a finite subgroup H such one of the following holds.*

- (i) H is a 2-fragment or a reverse-2-fragment.
- (ii) Γ and Γ^- are faithful Cauchy graphs and there exists an element a , such that $H \cup Ha$ is a 2-atom or a reverse-2-atom.

Proof. By Theorem 7.2, one of the following conditions holds:

- (1) One of the graphs Γ and Γ^- is not a Cauchy graph. By Theorem 8.3, the 1-atom containing 1 is a subgroup or the 1-atom containing 1 is a subgroup, and clearly (i) holds using Lemma 3.1.
- (2) One of the graphs Γ and Γ^- is non-faithful and its reverse-2-super-fragment is a block. The two cases are similar and each of them follows from the other applied to S^{-1} . Consider the case where Γ is non-faithful and take a reverse-super-fragment K , with $1 \in K$. By Lemma 8.2, K is a subgroup. Now (i) holds with $H = K$.
- (3) No vertex is incident to three distinct 2-atoms and to three distinct reverse-2-atoms. The two cases are similar and each of them follows from the other applied to S^{-1} . Consider the case where no vertex is incident to three distinct 2-atoms.

Let A be a 2-atom containing 1. It follows that the $\{a^{-1}A; a \in A\}$ consists of 2-atoms incident to 1. This family contains at most two distinct subsets. By Lemma 8.2, $A = Q \cup Qa$, for some a .

- (iii) The 2-atoms or the reverse-2-atoms have cardinality 2. The result holds in this case with $H = \{1\}$. \square

The next special case is enough for most of the applications:

Theorem 8.5. *Let S be finite generating subset of a group G with $1 \in S$ and $|S| < (1 - \frac{1}{p})|G| + 1$, where p denotes the smallest cardinality of a finite non-null subgroup of G , if G is a torsion group, and $p = \infty$ otherwise.*

Also assume that Γ is degenerate and reverse-degenerate, where $\Gamma = \text{Cay}(G, S)$. Then either S is a progression or there are a finite subgroup H with $|H| \geq 2$ such one of the following holds.

- (i) H is a 2-fragment or a reverse-2-fragment,
- (ii) Γ and Γ^- are faithful Cauchy graphs and there exists an element a , such that $H \cup Ha$ is a 2-atom or a reverse-2-atom.

Proof. The result holds by Theorem 8.4, unless Γ and Γ^- are Cauchy graphs and the 2-atom has size 2 or the reverse-atom has size 2. The two cases are similar and each of them follows from the other applied to S^{-1} . Consider the case where a 2-atom has the form $\{1, r\}$. We have $|\{1, r\}S| = |S| + 1$. Decompose $S = S_1 \cup \dots \cup S_m$, where S_1, \dots, S_m are right r -progression such that m is minimal. In particular, rS_i contains one element not contained in S , for all $1 \leq i \leq m$. Without loss of generality, we may assume that $|S_1| \leq \dots \leq |S_m|$. If $m = 1$, then S is a progression and (i) holds. Assume that $m \geq 2$ and let K be the subgroup generated by r . We have $|S_2| = |K|$,

otherwise

$$|S| + 1 = |\{1, r\}S| \geq |\{1, r\}S_1| + |\{1, r\}S_2| + |S \setminus (S_1 \cup S_2)| \geq |S| + 2.$$

In particular, K is a proper subgroup. Since $|S_2| = \dots = |S_m| = |K|$, we have also, $KS \neq G$, otherwise $|S| \geq |G| - |K| + 1 \geq (1 - \frac{1}{p})|G| + 1$, a contradiction. Now we have $|S| - 1 = \kappa_2 \leq |KS| - |K| = |S| + |K| - |S_1| - |K|$, and hence $|S_1| = 1$. In particular, $\kappa_2 = |KS| - |K|$, and thus the subgroup K is a 2-fragment. Therefore (ii) holds with $H = K$. \square

The last result generalizes a result proved in the abelian case in [6], and applied to the Frobenius problem in [9]. Our present condition $|S| < (1 - \frac{1}{p})|G| + 1$, is sharper than the condition $|S| < |G|/2 + 1$, used in [9].

We have also a description of degenerate Cayley graphs.

Corollary 8.6. *Let G be group and let S be finite generating subset with $1 \in S$. The following conditions are equivalent.*

(i) *There is a finite subset A with $|A| \geq 2$,*

$$\min(|AS|, |SA|) \leq \min(|G| - 2, |A| + |S| - 1).$$

(ii) *There are a finite subgroup H and an element a , such that*

$$\min(|H\{1, a\}S|, |S\{1, a\}H|) \leq \min(|G| - 2, 2|H| + |S| - 1).$$

Proof. Put $\text{Cay}(G, S)$. Clearly, $\Gamma^- = \text{Cay}(G, S^{-1})$. Clearly (i) implies (ii). Using Theorem 8.4, we see easily that (ii) implies (i).

9. ADDITIVE COMBINATORICS

Recall a well known fact:

Lemma 9.1. *(folklore) Let a, b be elements of a group G and let H be a finite subgroup of G . Let A, B be subsets of G such that $A \subset aH$ and $B \subset Hb$. If $|A| + |B| > |H|$, then $AB = aHb$.*

Lemma 9.2. *Let S be finite generating subset of a group G with $1 \in S$. Assume that the graph $\Gamma = \text{Cay}(G, S)$ is degenerate and let H be a subgroup which is a 2-fragment.*

Then $S^{-1}HS = S^{-1}S \cup a^{-1}Ha$, for some $a \in S$.

Proof. Put $|HS| = k|H|$ and take a partition $S = S_1 \cup \dots \cup S_k$, where S_i is the trace of S on some right coset of H . We shall assume that $|S_1| \leq \dots \leq |S_k|$.

Observe that $k \geq 2$, since H is a proper subgroup and since $1 \in S$. By the definitions, we have $|S| - 1 \geq \kappa_2(S) = |HS| - |H|$. Thus, $2|H| - |S_1| - |S_2| \leq$

$|HS| - |S| \leq |H| - 1$. Therefore $|H| + 1 \leq |S_1| + |S_2|$. Now for every couple $(i, j) \in [1, k] \times [1, k] \setminus \{(1, 1)\}$, we have

$$|H| + 1 \leq |S_1| + |S_2| \leq |S_i| + |S_j|,$$

and hence by Lemma 9.1,

$$S^{-1}S \supset S_i^{-1}S_j = S_i^{-1}HS_j.$$

Take an element $a \in S_1$. We have $S^{-1}S \cup a^{-1}Ha = S^{-1}HS$. \square

Proof of Theorem 1.1 Assume that A is not a progression.

Put $S = r^{-1}A$, where $r \in A$. Since $S \subset A^{-1}A$, we have $\langle S \rangle \subset G$. The other inclusion follows since $S^{-1}S = A^{-1}A$. Notice that $1 \in S$ and that S generates G . Put $\Gamma = \text{Cay}(G, S)$.

If $S^{-1}S = G$ or $SS^{-1} = G$, then (ii) holds with $H = G$.

If $|S^{-1}S| = 2|G| - 1$, then $S^{-1}S = G \setminus \{u\}$, for some u . Since $S^{-1}S$ is a self-reverse set, we have $u^2 = 1$. Thus (i) holds. Similarly (i) holds, if $|SS^{-1}| = |G| - 1$.

So we may assume that $|S| \geq 2$, $|SS^{-1}|, |S^{-1}S| \leq |G| - 2$. By Lemma 9.1, $2|S| \leq |G|$. Clearly, Γ is degenerate and reverse-degenerate.

Claim G has a subgroup which is a 2-fragment or a reverse 2-fragment.

Suppose the contrary. By Theorem 8.5, Γ and Γ^- are faithful Cauchy graphs and there exists an element e , such that $H \cup He$ is a 2-atom or a reverse-2-atom, where H is a non-null subgroup. The two cases are similar and each of them follows from the other applied with S^{-1} replacing S . So we shall deal only with the case where $H \cup He$ is a 2-atom.

Since Γ is a Cauchy graph and by the assumptions, we have $2|S| > |S^{-1}S| \geq 2|S| - 1$. Thus, S^{-1} is a 2-fragment.

Take a partition $S = S_1 \cup \dots \cup S_k$, where S_i is the trace of S on some right coset of H . We shall assume that $|S_1| \leq \dots \leq |S_k|$. By Lemma 8.1, one may take $1 \in S_1$. Assume first that $|S_1| < |H|$. It follows that $H \cup He$ is not a subset of S^{-1} . By Theorem 5.1, $(H \cup He) \cap S^{-1} = \{1\}$, contradicting Lemma 3.4. Thus $|S_1| = |H|$, and hence $HS = S$. In particular, $|HS| - |H| \leq |S| - |H|$, and Γ would not be a Cauchy graph, a contradiction proving the claim.

Case 1. G has a subgroup H which is a 2-fragment.

By Lemma 9.2, $S^{-1}HS = S^{-1}S \cup b^{-1}Hb$, for some $b \in S = r^{-1}A$. Therefore, $A^{-1}rHr^{-1}A = A^{-1}A \cup b^{-1}Hb$, for some $b \in S = r^{-1}A$. In particular, (ii) holds.

Case 2. G has a subgroup which is a reverse 2-fragment.

By Lemma 9.2, $SHS^{-1} = SS^{-1} \cup bHb^{-1}$, for some $b \in S = r^{-1}A$. Thus, $r^{-1}AHA^{-1}r = r^{-1}AA^{-1}r \cup bHb^{-1}$, In particular, (iii) holds. \square

Acknowledgement The author would like to thank Professors Ben Green and Terence Tao, for calling his attention to Freiman's work and Husbands dissertation.

REFERENCES

- [1] A. Cauchy, Recherches sur les nombres, *J. Ecole polytechnique* 9(1813), 99-116.
- [2] H. Davenport, On the addition of residue classes, *J. London Math. Soc.* 10(1935), 30-32.
- [3] G. T. Diderrich, On Kneser's addition theorem in groups, *Proc. Amer. Math. Soc.* (1973), 443-451.
- [4] G. Freiman, Groups and the inverse problems of additive number theory. (Russian), *Number-theoretic studies in the Markov spectrum and in the structural theory of set addition* (Russian), pp. 175-183. Kalinin. Gos. Univ., Moscow, 1973.
- [5] Y. O. Hamidoune, Sur les atomes d'un graphe orienté, *C. R. Acad. Sc. Paris A* 284 (1977), 1253-1256.
- [6] Y. O. Hamidoune, On subsets with a small sum in abelian groups I: The Vosper property, *Europ. J. of Combinatorics* 18 (1997), 541-556.
- [7] Y. O. Hamidoune, An isoperimetric method in additive theory. *J. Algebra* 179 (1996), no. 2, 622-630.
- [8] Y. O. Hamidoune, On small subset product in a group. Structure Theory of set-addition, *Astérisque* no. 258(1999), xiv-xv, 281-308.
- [9] Y. O. Hamidoune, Some results in Additive number Theory I: The critical pair Theory, *Acta Arith.* 96, no. 2(2000), 97-119.
- [10] Y. O. Hamidoune, Some additive applications of the isoperimetric approach, *Annales de l'Institut Fourier* 58(2008), fasc. 6, 2007-2036. .
- [11] Y. O. Hamidoune, A Structure Theory for Small Sum Subsets, Preprint, 2009.
- [12] Y. O. Hamidoune, Two Inverse results related to a question of Tao, Prprint 2010.
- [13] L. Husbands, Approximate Groups in Additive Combinatorics: A Review of Methods and Literature, *Master's dissertation*, University of Bristol, September, 2009.
- [14] J. H. B. Kemperman, On small sumsets in Abelian groups, *Acta Math.* 103 (1960), 66-88.
- [15] M. Kneser, Summenmengen in lokalkompakten abelschen Gruppen, *Math. Zeit.* 66 (1956), 88-110.
- [16] H. B. Mann, An addition theorem for sets of elements of an Abelian group, *Proc. Amer. Math. Soc.* 4 (1953), 423.
- [17] J. E. Olson, On the symmetric difference of two sets in a group, *Europ. J. Combinatorics*, (1986), 43-54.
- [18] O. Serra and G. Zémor, Large sets with small doubling modulo p are well covered by an arithmetic progression. *Ann. Inst. Fourier (Grenoble)* 59 (2009), no. 5, 2043-2060.
- [19] T. Tao, Open question: noncommutative Freiman theorem, <http://terrytao.wordpress.com/2007/03/02/open-question-noncommutative-freiman-theorem>.
- [20] T. Tao, An elementary non-commutative Freiman theorem, <http://terrytao.wordpress.com/2009/11/10/an-elementary-non-commutative-freiman-theorem>.
- [21] T. Tao, V. H. Vu, *Additive Combinatorics*, Cambridge Studies in Advanced Mathematics 105 (2006), Cambridge University Press.
- [22] G. Vosper, The critical pairs of subsets of a group of prime order, *J. London Math. Soc.* 31 (1956), 200-205.
- [23] V. H. Vu and P. M. Wood, The inverse Erdős-Heilbronn problem, *Electron. J. Combin.* 16 (2009), no. 1, Research Paper 100, 8 pp.

UPMC UNIV PARIS 06, E. COMBINATOIRE,, CASE 189, 4 PLACE JUSSIEU, 75005
PARIS, FRANCE

E-mail address: `hamidoune@math.jussieu.fr`